DEPARTMI **8320-01**

48 CFR Parts 802, 804, 811, 812, 824, 839, and 852

RIN 2900-AQ41

VA Acquisition Regulation: Acquisition of Information Technology; and Other Contracts for Goods and Services involving Information, VA Sensitive Information, and Information Security; and Liquidated Damages Requirements for Data Breach

AGENCY: Department of Veterans Affairs.

ACTION: Proposed rule.

SUMMARY: The Department of Veterans Affairs (VA) is proposing to amend and update its VA Acquisition Regulation (VAAR) in phased increments to revise or remove any policy superseded by changes in the Federal Acquisition Regulation (FAR), to remove procedural guidance internal to VA into the VA Acquisition Manual (VAAM), and to incorporate any new agency specific regulations or policies. This rulemaking revises the VAAR by adding a part covering Acquisition of Information Technology and revising coverage concerning Other Contracts for Goods and Services involving mandatory information, privacy, and security requirements to include policy concerning VA Sensitive Personal Information, information security, and liquidated damages requirements for data breach in the following parts: Administrative and Information Matters; Describing Agency Needs; Protection of Privacy and Freedom of Information, as well as Acquisition of Commercial Items. It also revises affected parts concerning Definitions of Words and Terms, and Solicitation Provisions and Contract Clauses.

DATES: Comments must be received on or before **[Insert date 60 days after date of publication in the *FEDERAL REGISTER*]** to be considered in the formulation of the final rule.

ADDRESSES: Written comments may be submitted through www.Regulations.gov or mailed to Mr. Rafael Taylor, 003A2A, Department of Veterans Affairs, Procurement Policy and Warrant Management Services (PPS), 810 Vermont Avenue NW, 20420, Washington, DC 20420. Comments should indicate that they are submitted in response to "RIN 2900-AQ41—VA Acquisition Regulation: Acquisition of Information Technology; and Other Contracts for Goods and Services involving Information, VA Sensitive Personal Information, and Information Security, and Liquidated Damages Requirements for Data Breach." Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Mr. Rafael N. Taylor, Senior Procurement Analyst, Procurement Policy and Warrant Management Services, 003A2A, 810 Vermont Avenue NW, Washington, DC 20420, (202) 714-8560. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION:

Background

This rulemaking is issued under the authority of the Office of Federal Procurement Policy (OFPP) Act which provides the authority for an agency head to issue agency acquisition regulations that implement or supplement the FAR.

VA is proposing to revise the VAAR to add new policy or regulatory requirements, to update existing policy, and to remove any redundant guidance where it may exist in affected parts, and to place guidance that is applicable only to VA's internal operating processes or procedures in the VAAM. Codified acquisition regulations may be amended and revised only through rulemaking. All amendments, revisions, and removals have been reviewed and concurred with by VA's Integrated Product Team of agency stakeholders.

The VAAR uses the regulatory structure and arrangement of the FAR and headings and subject areas are consistent with the FAR content. The VAAR is divided into subchapters, parts (each of which covers a separate aspect of acquisition), subparts, sections, and subsections.

The Office of Federal Procurement Policy Act, as codified in 41 U.S.C. 1707, provides the authority for the Federal Acquisition Regulation and for the issuance of agency acquisition regulations consistent with the FAR.

When Federal agencies acquire supplies and services using appropriated funds, the purchase is governed by the FAR, set forth at title 48 Code of Federal Regulations (CFR), chapter 1, parts 1 through 53, and the agency regulations that implement and supplement the FAR. The VAAR is set forth at title 48 CFR, chapter 8, parts 801 through 873.

Discussion and Analysis

VA proposes to make the following changes to the VAAR in this phase of its revision and streamlining initiative. This rule adds a new VAAR part 839 along with proposed revisions to other parts as described below. Where necessary, procedural guidance has been considered for inclusion in VA's internal agency operating procedures in accordance with FAR 1.301(a)(2). Similarly, delegations of authorities will be included in the VA Acquisition Manual (VAAM) as internal agency guidance. These changes seek to streamline and align the VAAR with the FAR and remove outdated and duplicative requirements and reduce burden on contractors. The VAAM incorporates portions of the removed VAAR as well as other internal agency acquisition procedures. VA will rewrite certain parts of the VAAR and VAAM, and as VAAR parts are rewritten, will publish them in the Federal Register. VA will combine related topics, as appropriate. The VAAM is being created in parallel with these revisions to the VAAR and is not subject to the rulemaking process as the VAAM contains internal VA procedures and

guidance. Therefore, the VAAM will not be finalized and available online for any new parts until corresponding VAAR parts are finalized.

VAAR Part 802—Definitions of Words and Terms

VA proposes to add the following 11 definitions in section 802.101 to reflect terms VA uses in more than one part as related to the amendatory text, parts and clauses and provisions outlined in this VAAR case: Business Associate, Business Associate Agreement (BAA), Gray market items, Information system, Information technology, Information technology-related contracts, Privacy officer, Security plan, Sensitive personal information, VA Information Security Rules of Behavior for Organizational Users, and VA sensitive information.

VAAR Part 804—Administrative and Information Matters

We propose to add the following authorities to part 804:

- 38 U.S.C. 5723, which requires all users of VA information and information systems to 1) Comply with all VA security policies, procedures, and practices; 2) Take security awareness training on at least an annual basis; 3) Report all actual or suspected security and privacy incidents immediately to the Information System Security Officer (ISSO) or Privacy Officer of the facility and to their immediate supervisor (in VA contracts contractors will be required to report security incidents to the contracting officer and the contractor officer's representative (COR), as identified or directed in the contract, within one hour of discovery or suspicion); and 4) Sign and acknowledge VA's Information Security Rules of Behavior for Organizational Users (i.e., "VA National Rules of Behavior") on an annual basis;
- 38 U.S.C. 5724, which requires VA, in the event the Secretary determines there exists a reasonable risk for the potential misuse of sensitive personal information

involved in a data breach, to provide credit protection services, as well as notification to the affected individual; and

- 38 U.S.C. 5725(a)-(c), which requires the Secretary to ensure that if a contract is entered into for the performance of any Department function that requires access to sensitive personal information include, as a condition of the contract, that a contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract. This statute also requires the contractor, or any subcontractors under the contract, to promptly notify VA (within one hour of discovery or suspicion) of any actual or suspected data breach that occurs with respect to sensitive personal information. It further requires that each such contract is subject to liquidated damages to be paid by the contractor to VA in the event of a data breach of any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract. Such liquidated damages will be used for the purpose of VA providing credit protection services.

VA proposes to amend part 804 by adding subpart 804.19, Basic Safeguarding of Covered Contractor Information Systems, and sections 804.1900-70, Scope of subpart; 804.1902, Applicability; 804.1970, Information security policy—contractor general responsibilities; and 804.1903, Contract clause.

In section 804.1900-70, Scope of subpart, it would state that the subpart prescribes policies and procedures for information security and protection of VA information, information systems, and VA sensitive information, including sensitive personal information.

In section 804.1902, Applicability, VA stipulates that the subpart would apply to all VA acquisitions, including acquisitions of commercial items other than commercially

available off-the-shelf items, when a contractor's information system may contain VA information.

In section 804.1970, Information security policy—contractor general responsibilities, VA provides policy requiring contractors, subcontractors, business associates and their employees who are users of VA information or information systems, or have access to VA information and VA sensitive information to—

- Comply with all VA information security program policies, procedures, practices and related contract requirements, specifications and clauses;
- Complete VA security awareness training on an annual basis;
- Complete VHA's Privacy and Health Insurance Portability and Accountability Act of 1996 (HIPAA) Training on an annual basis when access to protected health information (PHI) is required;
- Report all actual or suspected security/privacy incidents and reporting information to the contracting officer, and COR as identified or as directed in the contract, within one hour of discovery or suspicion;
- Comply with VA policy as it relates to personnel security and suitability program requirements for background screening of both employees and non-employees who have access to VA information systems and data;
- Comply with directions that may be issued by the contracting officer or COR, or from the VA Assistant Secretary for Information and Technology or a designated representative through the contracting officer or COR, directing specific activities when a security/privacy incident occurs;
- Sign an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) as required by 38 U.S.C. 5723, FAR 39.105, Privacy, and clause 852.204-71, Information and Information Systems Security, on an

annual basis. The VA Information Security Rules of Behavior describe the responsibilities and expected behavior of contractors, subcontractors, business associates and their employees who are users of VA information or information systems, information assets and resources, or have access to VA information;

- Maintain records and compliance reports regarding HIPAA Security and Privacy Rule compliance in order to provide such information to VA upon request to ascertain whether the business associate is complying with all applicable provisions under both rules' regulatory requirements; and
- Flow down requirements in all subcontracts and Business Associate Agreements (BAAs), at any level, as provided in the clause at 852.204-71, Information and Information Systems Security.

Section 804.1903, Contract clause, would require contracting officers to insert clause 852.204-71, Information and Information Systems Security, as further described in VAAR part 852 below in the preamble, when FAR clause 52.204-1, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903.

VAAR Part 811—Describing Agency Needs

We propose to add the following authorities to supplement the existing authorities for the proposed policies and procedures under part 811 as follows:

- 38 U.S.C. 5723, which requires all users of VA information and information systems to 1) Comply with all VA security policies, procedures, and practices; 2) Take security awareness training on at least an annual basis; 3) Report all actual or suspected security and privacy incidents and report the information to the appropriate Information System Security Officer (ISSO) or Privacy Officer of the facility and to their immediate supervisor (in VA contracts contractors will be required to report security incidents to the contracting officer and the contractor

officer's representative (COR), as identified or directed in the contract, within one hour of discovery or suspicion); and 4) Sign and acknowledge VA's Information Security Rules of Behavior for Organizational Users (i.e., VA National Rules of Behavior) on an annual basis.

- 38 U.S.C. 5724, which requires VA, in the event the Secretary determines there exists a reasonable risk for the potential misuse of sensitive personal information involved in a data breach, to provide credit protection services, as well as notification to the affected individual.
- 38 U.S.C. 5725(a)-(c), which requires the Secretary to ensure that if a contract is entered into for the performance of any Department function that requires access to sensitive personal information include, as a condition of the contract, that a contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract. This statute also requires the contractor, or any subcontractors under the contract, to promptly notify VA (within one hour of discovery or suspicion) of any actual or suspected data breach that occurs with respect to sensitive personal information. It further requires that each such contract is subject to liquidated damages to be paid by the contractor to VA in the event of a data breach of any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract. Such liquidated damages will be used for the purpose of VA providing credit protection services.

We propose to add a new subpart 811.5, Liquidated damages, including underlying sections as follows:

We propose to add 811.500, Scope, that would provide that the subpart is to prescribe policies and procedures for using a liquidated damages clause in solicitations

and contracts that involve sensitive personal information. It also states that it pertains to any solicitations and contracts involving sensitive personal information issued by another agency for or on behalf of VA through an interagency acquisition in accordance with (IAW) FAR subpart 17.5 and VAAR subpart 817.5.

We propose to add 811.501-70, Policy—statutory requirement, that provides that contracting officers are required to include a liquidated damages clause pertaining to the protection of sensitive personal information in accordance with 38 U.S.C. 5725(b), to be paid by the contractor to the VA for the provision of credit protection services to affected individuals pursuant to 38 U.S.C. 5724(b) in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract.

We propose to add 811.503-70, Contract clause, that would prescribe new clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs, as described in the section describing the proposed revisions to part 852 in this preamble. The proposed clause would be required to be incorporated in VA solicitations, contracts, purchase orders, and other instruments (for both commercial and non-commercial acquisitions, as well as when using the procedures of FAR parts 8 and/or 12, or FAR part 13 as described in the Alternate versions of the clause), when access to sensitive personal information (as defined in 38 U.S.C. 5727 and in part 839) is required whether as a contractor, subcontractor, business associate or an employee of one of these entities. The clause—

- Would prohibit the disclosure of sensitive personal information to any other person or entity unless the disclosure is lawful and is expressly permitted under the contract;
- Would require contractors, subcontractors, business associates or their employees to promptly notify the contracting officer and the contracting officer's

representative (COR), of any security incident that occurs involving sensitive personal information; and

- Would require that if the contractor fails to protect sensitive personal information, the contractor shall, in the event of a data breach, in place of actual damages, pay to the Government liquidated damages per affected individual in an amount to be specified and inserted by the contracting officer in accordance with current VA internal policy. The amount to be inserted by the contracting officer would represent an estimate of the cost per affected individual for VA to provide credit protection services (e.g., notification, credit monitoring and related support) for individuals affected by a data breach.

VAAR Part 812—Acquisition of Commercial Items

We propose to amend 812.301, Solicitation provisions and contract clauses for the acquisition of commercial items, by removing a prescription for clause 852.212-70. This clause, which required contracting officers to review and check provisions and clauses that apply, has been removed as unnecessary and redundant to the normal selection process for provisions and clauses.

This section will also be amended by removing a prescription for clause 852.212-71, Gray Market Items, and to add prescriptions for two new clauses: 852.212-71, Gray Market and Counterfeit Items, and 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts. The new clauses were originally released as a VAAR Class Deviation and will be codified via this rule.

VAAR Part 824—Protection of Privacy and Freedom of Information

We propose to add the following authorities to part 824:

- 38 U.S.C. 5723, which requires all users of VA information and information systems to 1) Comply with all VA security policies, procedures, and practices; 2) Take security awareness training on at least an annual basis; 3) Report all actual

or suspected security and privacy incidents immediately to the Information System Security Officer (ISSO) or Privacy Officer of the facility and to their immediate supervisor (in VA contracts contractors will be required to report security incidents to the contracting officer and the contractor officer's representative (COR)), as identified or directed in the contract, within one hour of discovery or suspicion); and 4) Sign and acknowledge VA's Information Security Rules of Behavior for Organizational Users (i.e., "VA National Rules of Behavior") on an annual basis.

- 38 U.S.C. 5724, which requires VA, in the event the Secretary determines there exists a reasonable risk for the potential misuse of sensitive personal information involved in a data breach, to provide credit protection services, as well as notification to the affected individual.
- 38 U.S.C. 5725 (a)-(c), which requires the Secretary to ensure that if a contract is entered into for the performance of any Department function that requires access to sensitive personal information include, as a condition of the contract, that a contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract. This statute also requires the contractor, or any subcontractors under the contract, to promptly notify VA (within one hour of discovery or suspicion) of any actual or suspected data breach that occurs with respect to sensitive personal information. It further requires that each such contract is subject to liquidated damages to be paid by the contractor to VA in the event of a data breach of any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract. Such liquidated damages will be used for the purpose of VA providing credit protection services.

We propose to amend VAAR part 824 under subpart 824.1, Protection of Individual Privacy, by adding sections 824.103-70, Protection of privacy—general requirements and procedures related to Business Associate Agreements, and 824.103-71, Liquidated damages—protection of information.

We propose to add 824.103-70, Protection of privacy—general requirements and procedures related to Business Associate Agreements (BAAs), to establish policy. This would ensure compliance with unique responsibilities to protect protected health information, and require contractors performing under VA contracts subject to unique PHI and Health Insurance Portability and Accountability Act (HIPAA) to comply with requirements in this section. It describes the requirement for a Business Associate Agreement and when that applies. It describes that the Veterans Health Administration (VHA) is a HIPAA Covered Entity. VHA is the only administration of the Department of Veterans Affairs that is a HIPAA Covered Entity under the HIPAA Privacy Rule. It would further require that contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates. It also describes those instances where other components within VA Administrations may also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA. Basically, it would require contractors, subcontractors, and their employees, where HIPAA protected health information (PHI) is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized in order to perform certain health care operations activities or functions on behalf of the Veterans Health Administration (VHA) as a covered entity, to execute a BAA.

In 824.103-71, Liquidated damages—protection of information, it reinforces the applicability of a liquidated damages clause as prescribed at 811.503-70 when performance under a contract requires a contractor to enter into a business associate agreement with VHA because the contractor or its subcontractor is required to create, receive, maintain, or transmit VHA PHI or is required to store, generate, access, exchange, process, or utilize PHI, for certain services or functions, on behalf of VHA. The liquidated damages clause would be required to be added even in situations where the prime contractor never directly receives VA's sensitive personal information and the same flows directly to the prime contractor's subcontractor.

VAAR Part 839—Acquisition of Information Technology

We propose to add part 839, Acquisition of Information Technology, to implement and supplement FAR part 39, Acquisition of Information Technology, to incorporate, in consonance and together with the FAR, VA policies, procedures, and contract clauses necessary to control the relationship between VA and contractors or prospective contractors concerning unique aspects of the acquisition of information technology or service contracts related to information technology

We propose to include the following authorities as the authority for the proposed policies and procedures under part 839: 38 U.S.C. 5723; 5724; 5725(a)–(c); 40 U.S.C. 121(c); 40 U.S.C. 11319(b)(1)(C); 41 U.S.C. 1121(c)(3); 1303 and 1702; and 48 CFR 1.301-1.304. The authorities are described as follows—

- 38 U.S.C. 5723, which requires all users of VA information and information systems to 1) Comply with all VA security policies, procedures, and practices; 2) Take security awareness training on at least an annual basis; 3) Report all actual or suspected security and privacy incidents to the Information System Security Officer (ISSO) or Privacy Officer of the facility and to their immediate supervisor (in VA contracts contractors will be required to report security incidents to the

contracting officer and the contractor officer's representative (COR), as identified or directed in the contract, within one hour of discovery or suspicion); and 4) Sign and acknowledge VA's Information Security Rules of Behavior for Organizational Users (i.e., "VA National Rules of Behavior") on an annual basis;

- 38 U.S.C. 5724, which requires VA, in the event the Secretary determines there exists a reasonable risk for the potential misuse of sensitive personal information involved in a data breach, to provide credit protection services, as well as notification to the affected individual;
- 38 U.S.C. 5725(a)-(c), which requires the Secretary to ensure that if a contract is entered into for the performance of any Department function that requires access to sensitive personal information include, as a condition of the contract, that a contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract. This statute also requires the contractor, or any subcontractors under the contract, to promptly notify VA (within one hour of discovery or suspicion) of any actual or suspected data breach that occurs with respect to sensitive personal information. It further requires that each such contract is subject to liquidated damages to be paid by the contractor to VA in the event of a data breach of any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract. Such liquidated damages will be used for the purpose of VA providing credit protection services;
- 40 U.S.C. 121(c), which authorizes the head of each executive agency to issue orders and directives that the agency head considers necessary to carry out the FAR;

- 40 U.S.C. 11319(b)(1)(C), which stipulates that a covered agency other than the Department of Defense may not enter into a contract or other agreement for information technology or information technology services, unless the contract or other agreement has been reviewed and approved by the Chief Information Officer (CIO) of the agency, and that permits VA to use the governance processes of the VA to approve such a contract or other agreement if the VA CIO is included as a full participant in the governance processes. It also further permits that for a contract or agreement for a non-major information technology investment under this authority, the CIO may delegate the approval of the contract or agreement to an individual who reports directly to the CIO;
- 41 U.S.C. 1121(c)(3), which speaks to the authority of an executive agency under another law to prescribe policies, regulations, procedures, and forms for procurement that are subject to the authority conferred to the Administrator of the Office of Federal Procurement Policy, as well as other sections of Title 41, Public contracts, as cited in (c)(3);
- 41 U.S.C 1303, an updated positive law codification to reflect additional authority of the VA as an executive agency to issue regulations that are essential to implement Governmentwide policies and procedures in the agency, as well as to issue additional policies and procedures required to satisfy the specific needs of the VA;
- 41 U.S.C. 1702, which addresses the acquisition planning and management responsibilities of Chief Acquisition Officers and Senior Procurement Executives, to include implementation of unique procurement policies, regulations and standards of the executive agency; and
- 48 CFR 1.301 through 1.304, which authorizes agencies to issue acquisition regulations that implement or supplement the FAR.

We propose to add 839.000, Scope of part, stating that the purpose of the part is to prescribe acquisition policies and procedures for use in acquiring information technology supplies, services and systems, and that it applies to both VA procured information technology systems as well as Interagency Acquisitions defined in FAR part 17 and VAAR part 817.

We propose to add subpart 839.1—General, with no text, and with the following sections within the subpart:

We propose to add 839.101, Policy, which identifies directives, security requirements, procedures and guidance that apply to all VA contracts and to VA contractors and subcontractors providing products, and contractors, subcontractors, and third-parties, in the performance of contractual obligations to VA when providing information technology related services.

We propose to add 839.105, Privacy, as a header only with no text.

We propose to add 839.105-70, Business Associate Agreements, information technology-related contracts and privacy, to address a key requirement that business associate agreements shall be executed whether for VHA directly as the only VA "Covered Entity" or for other contracts and agreements issued by other VA administrations and staff offices in support of VHA where contractors, subcontractors, business associates and their employees may have to access, receive or create VA sensitive information or sensitive personal information, on behalf of VHA, in order to provide certain health care operation services. (See 802.101 for the definition of information technology-related contracts.)

We propose to add 839.105-71, Liquidated damages—protection of information in information technology related contracts, in contracts for goods and services, to address the statutory requirement to include a liquidated damages clause as prescribed

in 811.503-70(a) in contracts where access to sensitive personal information is provided by the VA or on its behalf.

We propose to add 839.106-70, Information technology security and privacy contract clauses, to prescribe the use of the following clauses:

In paragraph (a), contracting officers shall insert the clause at 852.239-70, Security Requirements for Information Technology Resources, and the clause 852.239-71, Information Technology Security Plan and Accreditation, in all solicitations, contracts and orders exceeding the micro-purchase threshold that include information technology services.

In paragraph (b), clause 852.239-72, Information System Design and Development, would be required to be inserted in solicitations, contracts, orders and agreements where services to perform information system design and development are required.

In paragraph (c), clause 852.239-73, Information System Hosting, Operation, Maintenance or Use, would be required to be inserted in solicitations, contracts, orders and agreements where services to perform information system hosting, operation, maintenance or use are required.

In paragraph (d), clause 852.239-74, Security Controls Compliance Testing, would be required to be inserted in solicitations, contracts, orders and agreements when the clauses at 852.239-72 or 852.239-73 are inserted.

We propose to add subpart 839.2—Information and Communication Technology, with no text, and the following sections within the subpart.

We propose to add 839.201, Scope of subpart, to state that the subpart applies to all procurement of information and communication technology (ICT) supplies, services, and information and to require compliance with Section 508 standards.

Section 508 standards now refer to ICT in lieu of electronic and information technology, so VA is adopting the same terminology.

We propose to add 839.203, Applicability, to require submission of a VA Section 508 Checklist when required in VA solicitations, and to provide a website to help businesses ensure compliance with VA Section 508 Standards. This would assist VA in the evaluation of offeror's proposals when an acquisition involves the acquisition of information technology or the furnishing of services related to acquisition of information technology as defined in this part. The form will be available either in solicitations or via the website link identified.

We propose to add 839.203-70, Information and communication technology accessibility standards—contract clause and provisions, to prescribe new solicitation provision 852.239-75, Information and Communication Technology Accessibility Notice, and new contract clause 852.239-76, Information and Communication Technology Accessibility, which requires the use of the VA Section 508 Checklists.

VAAR Part 852—Solicitation Provisions and Contract Clauses

We propose to add clause 852.204-71, Information and Information Systems Security, that would require contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related contracts (see 802.101), shall adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA

Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems. It would describe in detail requirements for access to VA information and VA information systems and appropriate security and protection requirements; information on requirement for contractor operations in the United States; Contractor/subcontractor employee reassignment and termination notification requirements; VA information custodial requirements to include release, publication, and use of data, as well as media sanitization requirements; data retention, destruction and contractor self-certification requirements and use and copying of VA data and information; information with respect to violation of information custodial requirements, encryption, firewall and web services security controls, and disclosure of VA data and information. The clause also would cover compliance with privacy statutes and applicable regulations, as well as the requirement to report known or suspected security or privacy incidents. It further describes security incident investigation requirements and data breach notification requirements. It goes on to detail specific annual training requirements and the requirement to complete and such mandatory training requirements and complete acknowledgement of the VA Information Security Rules of Behavior for Organizational Users. A specific subcontract flow down requirement is also included.

We propose to add clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs, that provides that if the contractor fails

to protect VA sensitive personal information which results in a data breach, the contractor shall, in place of actual damages, pay to the Government liquidated damages in an amount per affected individual, inserted by the contracting officer based on internal VA policy, in order to cover costs related to notification, data breach analysis and credit monitoring for such individuals. In the event the contractor provides payment of actual damages in an amount determined to be adequate by the contracting officer, the contracting officer may forgo collection of liquidated damages. The contracting officer would insert Alternate I in all solicitations or contracts, in commercial items acquisitions awarded under the procedures of FAR part 8 or FAR part 12, and would insert Alternate II in all solicitations, contracts, or orders, in simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial items awarded under the procedures of FAR part 13 (see FAR 13.302-5(d)(1) and the clause at FAR 52.213-4).

We propose to remove clause 852.212-70, Provisions and Clauses Applicable to VA Acquisition of Commercial Items, as redundant to other FAR clauses.

We propose to remove clause 852.212-71, Gray Market Items, and to add a new clause in its place, 852.212-71, Gray Market and Counterfeit Items. This new clause would require that no used, refurbished, or remanufactured supplies or equipment/parts shall be provided. It would state that any procurement where the clause is inserted is for new Original Equipment Manufacturer (OEM) items only. No gray market items shall be permitted to be provided. The clause would also specify that no counterfeit supplies or equipment/parts shall be provided. Unlawful or unauthorized substitutions are set forth in the clause and include used items represented as new, or the false

identification of grade, serial number, lot number, date code, or performance characteristics. The clause would also require that all vendors under the solicitation or contract shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system, and would be required to be verified by an authorization letter or other documents from the OEM.

We propose to add 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts. This new clause would permit used, refurbished, or remanufactured parts to be provided. However, no gray market supplies or equipment shall be permitted to be provided. The clause would also require that no counterfeit supplies or equipment shall be provided. The clause would also require that all vendors shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system and would be required to be verified by an authorization letter or other documents from the OEM. Both proposed clauses are VA clauses that were originally released via a Class Deviation that we propose for codification as a part of this rulemaking.

We propose to add clause 852.239-70, Security Requirements for Information Technology Resources, to specify that contractors shall be responsible for information technology security for all systems connected to a Department of Veterans Affairs (VA) network or operated by the contractor for VA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the contractor has physical or electronic access to VA information that directly supports the mission of VA. Examples of tasks that require security provisions include—

(1) Hosting of VA e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by VA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to VA general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

The clause would also require the contractor to develop, provide, implement, and maintain an Information Technology Security Plan. This plan shall describe the processes and procedures that the contractor will follow to ensure appropriate security of information technology resources developed, processed, or used under this contract. The clause would require that within 30 days after contract award, the contractor shall submit the Information Technology Security Plan to the contracting officer for review. This plan shall detail the approach contained in the offeror's proposal, sealed bid or quotation. Upon acceptance by the contracting officer, the Plan will be incorporated into the contract by contract modification. As required by current VA policy, the contractor shall submit written proof of information technology security accreditation to the contracting officer. It also specifies specifically as pertains to information technology related contracts that its employees performing services under this contract complete VA security awareness training on an annual basis. This includes signing an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) as required by 38 U.S.C. 5723; FAR 39.105, Privacy; clause 852.204-71, Information and Information Systems Security, and this clause on an annual basis.

We propose to add provision 852.239-71, Information Technology Security Plan and Accreditation, that would require that all offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 852.239-70, Security Requirements for Information Technology Resources.

We propose to add clause 852.239-72, Information System Design and Development, which would be required in all solicitations, contracts, purchase orders and agreements where services to perform information system design and development are required. The contractor/subcontractor shall comply with the Privacy Act of 1974 (the Act)) and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies— (1) the Systems of Records (SOR); and (2) the design, development, or operational work that the contractor/subcontractor is to perform. During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

We propose to add clause 852.239-73, Information System Hosting, Operation, Maintenance, or Use, which would be required in all solicitations, contracts, purchase orders and agreements where services to perform information system hosting, operation, maintenance or used are required. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy handbooks, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security

control procedures must be equivalent to or exceed, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the contracting officer's representative (COR) and approved by VA Privacy Service prior to approval to operate. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the Privacy Impact Assessment and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII. The contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Electronic copies of the assessment must be provided to the COR. Media (e.g., hard drives, optical disks, CDs, back-up tapes) used by the contractor/ subcontractor that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per VA Directive 6500 requirements and as required by current VA policy. This must be completed within 30 days of termination of the contract.

We propose to add clause 852.239-74, Security Controls Compliance Testing, which would be required in solicitations, contracts, orders and agreements, when the clauses at 852.239-72 or 852.239-73 are inserted. Clause 852.239-73 would provide notice that VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by a contractor under the clauses contained within the contract. Clause 852.239-73 provides that with 10 working-days' notice, at the request of VA, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed,

operated, maintained, or used on behalf of VA, including those initiated by the Office of the Inspector General. VA may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by VA in the event of a security incident or at any other time.

We propose to add solicitation provision 852.239-75, Information Communication and Technology Accessibility Notice, and clause 852.239-76, Information and Communication Technology Accessibility, that require the use of the VA Section 508 Checklists to be submitted under solicitations and contracts, and that provide additional information regarding the VA Section 508 website.

Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, and other advantages; distributive impacts; and equity). E.O. 13563 (Improving Regulation and Regulatory Review) emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. The Office of Information and Regulatory Affairs has determined that this rule is not a significant regulatory action under Executive Order 12866.

The Regulatory Impact Analysis associated with this rulemaking can be found as a supporting document at www.regulations.gov.

Paperwork Reduction Act

This proposed rule includes provisions constituting collections of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) that require

approval by the Office of Management and Budget (OMB). Accordingly, under 44 U.S.C. 3507(d), VA has submitted a copy of this rulemaking action to OMB for its review.

OMB assigns control numbers to collections of information it approves. VA may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. VA is describing four groups of new collections of information in this rule under the Paperwork Reduction Act of 1995 for four separate OMB Control Numbers related to—

VAAR Part 804 related information collection:

1. Proposed clause, 852.204-71, Information and Information Systems Security, and section 804.1970, Information security policy—contractor general responsibilities.

VAAR Part 811 related information collection:

2. Proposed section 811.503-70, Contract clause, and proposed clause 852.211-70, Liquidated Damages—Reimbursement for Data Breach Costs.

VAAR Part 812 related information collection:

3. Proposed section 812.301(f), Solicitation provisions and contract clauses for the acquisition of commercial items, and proposed clauses 852.212-71, Gray Market and Counterfeit Items, and 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts.

VAAR Part 839 related information collection:

4. Proposed section 839.106-70, Information technology security and privacy clauses, and proposed clauses 852.239-70, Security Requirements for Information Technology Resources; 852.239-72, Information System Design and Development; and 852.239-73, Information System Hosting, Operation, Maintenance or Use. If OMB does not approve the collections of information as requested, VA will immediately remove the

provisions containing a collection of information or take such other action as is directed by OMB.

Written comments and recommendations for the proposed collections of information should be sent within 60 days of publication of this proposed rule through Federal Docket Management System (FDMS) at www.Regulations.gov or to Rafael Taylor, Office of Acquisition & Logistics, Procurement Policy & Warrant Management Services (003A2A), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or email to rafael.taylor@va.gov.

OMB is required to make a decision concerning the collections of information contained in this proposed rule between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication. This does not affect the deadline for the public to comment on the proposed rule.

The Department considers comments by the public on proposed collections of information in—

• Evaluating whether the proposed collections of information are necessary for the proper performance of the functions of the Department, including whether the information will have practical utility;

• Evaluating the accuracy of the Department's estimate of the burden of the proposed collections of information, including the validity of the methodology and assumptions used;

• Enhancing the quality, usefulness, and clarity of the information to be collected; and

• Minimizing the burden of the collections of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or

other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

The collections of information contained in this proposed rule at 48 CFR chapter 8 are described specifically and immediately following this paragraph, under their respective titles.

VAAR Part 804 related collections of information:

The collection of information contained in proposed clause, 852.204-71, Information and Information Systems Security and new section 804.1970, Information security policy—contractor general responsibilities, is described immediately following this paragraph.

Summary of collection of information:

We propose the use of clause 852.204-71, Information and Information Systems Security, as prescribed at 804.1903; and propose section 804.1970, Information security policy—contractor general responsibilities.

New proposed section 804.1970 and VAAR clause 852.204-71, Information and Information System Security, would require contractors, subcontractors, their employees, third-parties, and business associates who perform under a contract with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, to be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security. The clause and information collection requirement would be inserted in solicitations, contracts, purchase orders and agreements where VA information, VA sensitive information (including sensitive personal information or protected health information (PHI)), when the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, is required to be included in accordance with FAR 4.1903.

Description of need for information and proposed use of information:

This information collection requirement is needed to protect the safety and health of the nation's Veterans and to protect the security and integrity of VA information and VA sensitive information.

Clause 852.204-71 and section 804.1970 contain the following information collection requirements from the public:

Information Collection Requirement	Clause/Section
Contractor/subcontractor employee reassignment and termination notification	852.204-71
Report of known or suspected security/privacy incident and data breach	852.204-71, 804.1970
Provide an annual training certificate	852.204-71
Submission of data retention, destruction plan and contractor self-certification	852.204-71
Maintain records and compliance reports regarding HIPAA security and privacy rule compliance	804.1970
Submission of a detailed security plan	852.204-71
Report of all requests for, demands for production of, or inquiries, including court orders, about VA information and information systems	852.204-71

Total Burden Hours: 4,069

Total Number of Respondents: 8,223

Average Number of Respondents: 1,175

Total Annual Responses: 8,223

Average Annual Responses: 1,175

Total estimated annual cost to all respondents: $189,371 (4,069 hours at $46.54 per hour). This is based on the Bureau of Labor Statistics May 2020 Occupational Employment and Wages code "15-1231 Computer Network Support Specialists" mean hourly wage of $34.16 plus 36.25% fringe benefits per OMB Memo M-08-13 dated March 11, 2008.

VA gathered data for FY 2018, 2019 and 2020 across 11 North American Industry Classification System (NAICS) where such information collection requirements may be inserted into solicitations and contracts. Then VA looked at the types of

information collection requirements or burden may be required by the clause. Of the potential pool of previously awarded contracts (to both large and small businesses) during the three fiscal years where the proposed clause would be required to be included in solicitations and resulting contracts, VA calculated the average number of contracts awarded during the three fiscal years. We then used the average number of awards and estimated that for the purpose of identifying any potential information collection burden for contractor/subcontractor employee reassignment and termination notification of information collection requirements, only 45% would contain potential information collection requirements. The remaining information collection requirement categories are estimated as follows:

- VA estimates that 30% of the average number of contracts awarded during the three fiscal years in the identified 6 of 11 NAICS codes would require the clause and potential information collection requirement for report of known or suspected security/privacy incident and data breach.
- VA estimates that 100% of the average number of contracts awarded during the three fiscal years in the identified NAICS codes would require the clause and potential information collection requirement for the contractor/subcontractor employee training and certificates, and would be applicable when employees are onboarded by contractors.
- VA estimates no more than 15% of the average number of contracts awarded during the three fiscal years in the identified NAICS codes would require the clause and potential information collection requirement for the submission of data retention, destruction plan and contractor self-certification.
- VA estimates that 100% of the average number of contracts awarded during the three fiscal years in the identified eight of 11 NAICS codes would require the clause

and potential information collection requirement for maintain records and compliance reports regarding HIPAA security and Privacy Rule compliance.

• VA estimates that 100% of the average number of contracts awarded during the three fiscal years in the identified NAICS codes would require the clause and potential information collection requirement for the submission of a detailed security plan.

• VA estimates no more than 5% of the average number of contracts awarded during the three fiscal years in the identified NAICS codes that would require the clause and potential information collection requirement for the report of all requests for, demands for, production of, or inquiries, including court orders, about VA information and information systems, would be applicable.

Contractor/subcontractor employee reassignment and termination notification.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
1,357	1	5		113

Report of known or suspected security/privacy incident and data breach.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
807	1	180		2,421

Submission of contractor/subcontractor employee annual training certificate.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
3,016	1	2		101

Submission of data retention, destruction plan and contractor self-certification.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
452	1	5		38

Maintain records and compliance reports regarding HIPAA security and privacy rule compliance.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
2,138	1	30		1,069

Detailed security plan submission.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
302	1	60		302

Report of all requests for, demands for, production of, or inquiries, including court orders, about VA information and information systems.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
151	1	10		25

VAAR Part 811 related collections of information:

The collections of information contained in section 811.503-70, Contract clause and proposed clause 852.211-70, Liquidated Damages-Reimbursement for Data Breach Costs is described immediately following this paragraph.

Summary of collection of information:

We propose the use of clause 852.211-70, Liquidated Damages-Reimbursement for Data Breach Costs, as prescribed at 811.503-70, Contract clause, for sensitive personal information that will be created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized by a contractor, subcontractor, business associate, or an employee of one of these entities. This new proposed VAAR clause 852.211-70 requires the contractor, subcontractor, their employees or business associates to notify the VA through the contracting officer and

the contracting officer's representative (COR) of any security incident that occurs involving sensitive personal information.

Description of need for information and proposed use of information:

This information collection requirement is needed to protect the safety and health of the nation's Veterans and to protect the security and integrity of VA information and VA sensitive information.

Total Burden Hours: 6.5

Average Number of Respondents: 13

Average Annual Responses: 13

Total estimated annual cost to all respondents: $308 (6.5 hours at $47.42 per hour). This is based on the Bureau of Labor Statistics May 2020 Occupational Employment and Wages code "13-1020 Buyers and Purchasing Agents" mean hourly wage of $34.80 plus 36.25% fringe benefits per OMB Memo M-08-13 dated March 11, 2008.

VA gathered data for FY 2018, 2019 and 2020 across six North American Industry Classification System (NAICS) where such information collection requirements may be inserted into solicitations and contracts. Then VA looked at the types of information collection requirements or burden (i.e., notify the VA through the contracting officer and the contracting officer's representative of any security incident that occurs involving sensitive personal information.) Of the potential pool of previously awarded contracts during the average of the three fiscal years, VA calculated a rough estimate that 20% of six NAICS codes of past contract awards could be reasonably calculated as a rough estimate of a potential information collection requirement for any such contracts awarded to both large and small businesses.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours

13	1	30		6.5

VAAR Part 812 related collections of information:

The collections of information contained in section 812.301(f), Solicitation provisions and contract clauses for the acquisition of commercial items, and proposed clauses 852.212-71, Gray Market and Counterfeit Items, and 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts, are described immediately following this paragraph, under their respective titles.

Summary of collection of information:

We propose the use of clauses 852.212-71, Gray Market and Counterfeit Items, and 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts, as prescribed at 812.301(f), Solicitation provisions and contract clauses for the acquisition of commercial items.

New proposed VAAR clause 852.212-71, Gray Market and Counterfeit Items, require that no used, refurbished, or remanufactured supplies or equipment/parts shall be provided. It would state that any procurement where the clause is inserted is for new Original Equipment Manufacturer (OEM) items only. No gray market items shall be permitted to be provided. The clause would also specify that no counterfeit supplies or equipment/parts shall be provided. Unlawful or unauthorized substitutions are set forth in the clause and include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics. The clause would also require that all vendors shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system and would be required to be verified by an authorization letter or other documents from the OEM.

New proposed VAAR clause 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts, would permit

used, refurbished, or remanufactured parts to be provided under the solicitation and contract. However, no gray market supplies or equipment shall be permitted to be provided. The clause would also require that no counterfeit supplies or equipment shall be provided. The clause would also require that all vendors shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system and would be required to be verified by an authorization letter or other documents from the OEM.

Description of need for information and proposed use of information:

To prevent the inadvertent acquisition of gray market and counterfeit medical equipment, medical supplies, and IT equipment and to protect the VA supply chain.

The two clauses containing collections of information are described below:

Clause 852.212-71, Gray Market and Counterfeit Items, is required in solicitations and contracts for new medical supplies, new medical equipment, new information technology equipment, and maintenance of medical or information technology equipment that includes replacement parts if used, refurbished, or remanufactured parts are unacceptable, when the associated solicitation includes FAR provisions 52.212-1, Instruction to Offerors-Commercial Items, and 52.212-2, Evaluation-Commercial Items.

Clause 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts, is required in solicitations and contracts for the maintenance of information technology equipment that includes replacement parts, if used, refurbished, or remanufactured parts are acceptable, when the associated solicitation includes FAR provisions 52.212-1, Instruction to Offerors-Commercial Items, and 52.212-2, Evaluation-Commercial Items.

Total estimated burden hours: 2,170

Estimated average number of respondents: 4,342

Total estimated annual responses: 13,026

Total estimated annual cost to all respondents: $102,902 (2,170 hours at $47.42 per hour). This is based on the Bureau of Labor Statistics May 2020 Occupational Employment and Wages code “13-1020 Buyers and Purchasing Agents” mean hourly wage of $34.80 plus 36.25% fringe benefits per OMB Memo M-08-13 dated March 11, 2008.

VA gathered data for FY 2017, 2018 and 2019 across seven North American Industry Classification System (NAICS) where such information collection requirements may be inserted into solicitations and contracts. Then VA looked at the types of information collection requirements or burden (i.e., submitting an authorization letter or other documents from the Original Equipment Manufacturer.) Of the potential pool of previously awarded contracts during the average of the three fiscal years, VA calculated a rough estimate the seven NAICS codes as follows: two at 10%, one at 15%, one at 20%, and three at 25% of the past contract awards that could be reasonably calculated as a rough estimate of a potential information collection requirement for any such contracts awarded to both large and small businesses. Additionally, VA estimated three proposals would be received for each awarded contract, with the presumption that in some cases VA may only have received one proposal, and in others, more than three.

Because both clauses require the same information collection, one if for new OEM items and the other for other-than-new-parts and assumes both clauses will not be included in one acquisition. Therefore, the number of respondents for each clause is 50% the total of all NAICS estimated respondents.

Clause 852.212-71, Gray Market and Counterfeit Items.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
2,171	3	10		1,085

Clause 852.212-72, Gray Market, and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
2,171	3	10		1,085

VAAR Part 839 related collections of information:

The collections of information contained in section 839.106-70 and part 852 at proposed clauses 852.239-70, 852.239-72, and 852.239-73, are described immediately following this paragraph, under their respective titles.

Summary of collection of information:

We propose the use of 852.239-70, Security Requirements for Information Technology Resources; 852.239-72, Information System Design and Development, and 852.239-73, Information System Hosting, Operation, Maintenance, or Use, as prescribed at 839.106-70, Information technology security and privacy clauses.

New proposed clause 852.239-70, Security Requirements for Information Technology Resources, would require contractors, subcontractors, business associates and their personnel, when accessing VA information and or information systems in order to perform under a contract, to be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security. The clause and information collection requirement would be inserted in solicitations, contracts, purchase orders and agreements where VA information, VA sensitive information (including sensitive personal information or protected health information (PHI))—

(1) Is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized by a VA contractor,

subcontractor or third-party servicers or associates, or on behalf of any of these entities, in the performance of their contractual obligations to VA;

(2) By or on behalf of any of the entities identified in this section, regardless of—

(i) Format; or

(ii) Whether it resides on a VA or a non-VA system, or with a contractor, subcontractor, or third-party system or electronic information system(s), including cloud services, operating for or on the VA's behalf or as required by contract.

New proposed clause 852.239-72, Information System Design and Development, is required in all solicitations, contracts, orders and agreements where services to perform information system design and development are required.

New proposed clause 852.239-73, Information System Hosting, Operation, Maintenance, or Use, is required in all solicitations, contracts, orders and agreements for contracts where information systems are hosted, operated, maintained, or used on behalf of VA at non-VA facilities.

Description of need for information and proposed use of information:

Under the Federal Information Security Management Act (FISMA) (2002), section 3544(a)(1)(A)(ii), and the Federal Information Security Modernization Act of 2014, each agency of the Federal Government must provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. VA requires, based on Federal security requirements, that contractors and subcontractors, including business associates, and employees, that require access to VA information or information systems shall be subject to the same Federal laws, regulations, standards, policies and procedures as VA and VA personnel. This includes whenever it is accessed, maintained, processed, or utilized; or when VA information systems will be

designed or developed at non-VA facilities. These three clauses would enable VA to comply with its responsibilities under the Federal Information Security Modernization Act of 2014. The three clauses containing collections of information are described below:

Clause 852.239-70, Security Requirements for Information Technology Resources, is required in all solicitations, contracts, purchase orders, and agreements where VA sensitive information, including sensitive personal information is accessed, maintained, processed, or utilized as set forth in VAAR part 839. Contractors (including subcontractors, employees, and business associates) would be required to adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with personnel security program management and contract security in VA.

Clause 852.239-72, Information System Design and Development, is required in all solicitations, contracts, purchase orders and agreements where services to perform information system design and development are required. The contractor/subcontractor shall comply with the Privacy Act of 1974 (the Act) and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(1) The applicable and existing VA Privacy Act systems of records (SOR); and (2) the design, development, or operational work that the contractor/subcontractor is to perform. During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in

accordance with VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

Clause 852.239-73, Information System Hosting, Operation, Maintenance, or Use, is required in all solicitations, contracts, purchase orders and agreements where services to perform information system hosting, operation, or maintenance are required. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable HIPAA regulations, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy handbooks, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent to or exceed those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to approval to operate. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the Privacy Impact Assessment and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

The contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. Media (*e.g.*, hard drives, optical disks,

CDs, back-up tapes) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per VA Handbook 6500.1 requirements. This must be completed within 30 days of termination of the contract.

Section 839.101-70 and these three clauses require the contractor/subcontractor to submit the following information collections:

Information Collection Requirement	Clause/Section
Contractor/subcontractor employee reassignment and termination notification	852.239-70
Privacy Impact Assessment Report & Plan of Action and Milestones	852.239-72, 852.239-73
Maintain and provide information technology security plan	852.239-70
Submission of proof of information technology security accreditation	852.239-70
Verification of annual IT security plan validation	852.239-70
Submission of annual self-assessment	852.239-73
Report of any deficiencies on annual FISMA security controls assessment	852.239-73

Overall Total estimated burden hours: 4,815

Overall Estimated average number of respondents: 2,198

Overall Total estimated annual responses: 2,198

Total estimated annual cost to all respondents: $228,327 (4,815 hours at $47.42 per hour). This is based on the Bureau of Labor Statistics May 2020 Occupational Employment and Wages code “13-1020 Buyers and Purchasing Agents” mean hourly wage of $34.80 plus 36.25% fringe benefits per OMB Memo M-08-13 dated March 11, 2008.

VA gathered data for FY 2018, 2019 and 2020 across 11 North American Industry Classification System (NAICS) where such information collection requirements may be inserted into solicitations and contracts. Then VA looked at the types of information collection requirements or burden that may be required across the three VAAR part 839 clauses. Of the potential pool of previously awarded contracts (to both

large and small businesses) during the three fiscal years where the proposed clauses would be required to be included in solicitations and resulting contracts, VA calculated the average number of contracts awarded during the three fiscal years. We then used the average number of awards and estimated that for the purpose of identifying any potential information collection burden for Contractor/Subcontractor Employee Reassignment and Termination Notification of information collection requirements, only 45% would contain a potential information collection requirements. VA estimates that 100% of the average number of contracts awarded during the three fiscal years in the identified 11 NAICS codes would require the clause and potential information collection requirement for maintain and provide Information Technology Security Plan. Submission of proof of information technology security accreditation, and verification of annual IT security plan validation: VA also estimates 5% of the average number of contracts awarded during the three fiscal years in the identified 11 NAICS codes would require the clause and potential information collection requirement for report of any deficiencies on annual FISMA security controls assessment. Moreover, VA estimates that 100% of the average number of contracts awarded during the three fiscal years in six of the identified 11 NAICS codes would require the clause and potential information collection requirement for Privacy Impact Assessment report & Plan of Action and Milestones. Finally, VA estimates that 100% of the average number of contracts awarded during the three fiscal years in eight of the identified 11 NAICS codes would require the clause and potential information collection requirement for submission of annual self-assessment.

- 852.239-70, Security Requirements for Information Technology Resources.

  Total Burden Hours: 2,375

  Average Number of Respondents: 2,601

  Average Annual Responses: 2,601

Contractor/subcontractor employee reassignment and termination notification.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
1,357	1	5		113

Maintain and provide Information technology security plan.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
3,016	1	30		1,508

Submission of proof of information technology security accreditation.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
3,016	1	10		503

Verification of annual IT Security Plan validation.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
3,016	1	5		251

- 852.239-72, Information System Design and Development:

  Privacy Impact Assessment Report & Plan of Action and Milestones

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
1,345	1	30		673

  Total Burden Hours: 673

  Average Number of Respondents: 1,345

  Average Annual Responses: 1,345

- 852.239-73, Information System Hosting, Operation, Maintenance, or Use:

  Total Burden Hours: 1,767

Average Number of Respondents: 1,211

Average Annual Responses:1,211

Privacy Impact Assessment Report & Plan of Action and Milestones.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
1,345	1	30		673

Submission of annual self-assessment.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
2,138	1	30		1,069

Report of any deficiencies on annual FISMA security controls assessment.

No. of respondents	x No. of responses per respondent	x No. of minutes	÷ by 60	Number of Burden Hours
151	1	10		25

Regulatory Flexibility Act

The Secretary hereby certifies that this proposed rule would not have a significant economic impact on a substantial number of small entities as they are defined in the Regulatory Flexibility Act (5 U.S.C. 601–612). Therefore, pursuant to 5 U.S.C. 605(b), the initial and final regulatory flexibility analysis requirements of 5 U.S.C. 603 and 604 do not apply.

This rulemaking does not change VA's policy regarding small businesses and does not have a significant economic impact to individual businesses. The overall impact of the proposed rule would be of benefit to small businesses owned by Veterans or service-disabled Veterans as the VAAR is being updated to provide needed guidance to ensure VA's contractors properly protect and safeguard VA sensitive information,

which includes Veteran's sensitive personal information. This rulemaking adds a new VAAR part concerning Acquisition of Information Technology that codifies information collection burdens. VA's requirement to collect the information is the result of existing requirements to ensure compliance across the Federal government and specifically when VA contractors, subcontractors, business associates and their employees require access to VA information (including VA sensitive information) or information systems. VA is merely adding existing and current regulatory requirements to the VAAR and placing guidance that is applicable only to VA's internal operation processes or procedures into a VA Acquisition Manual. VA estimates no substantial cost impact to individual businesses will result from these rule updates already required to be considered by both large and small businesses to receive an award from VA or another Federal agency. There are costs associated with this rulemaking pertaining to the codification of an information collection request in order to comply with VA's responsibilities under the Federal Information Security Modernization Act of 2014. Each agency of the Federal Government must provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. By statute, VA is required to ensure that its contractors, subcontractors, business associates, and their employees operating under contracts at VA shall be subject to the same Federal laws, regulations, policies or procedures as VA and VA personnel. While this requirement adds some burden in annual costs and hours to firms already awarded and performing contracts at VA, the overall cost is considered *de minimis*, for either large or small contractors, in relation to the potential impact and harm to Veterans and VA information and information systems should a contractor not comply. Properly setting forth the requirements will provide clarity to the public and ensure appropriate safeguards are in place to ensure protection of VA's information (in particular VA

sensitive personal information) and information systems. In total, this rulemaking does not change VA's policy regarding small businesses, does not have a substantial economic impact to individual businesses, and does not significantly increase or decrease costs small business were already required to bear when performing contracts which required the access, maintenance, process, or utilization of VA sensitive information or information systems.

Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 requires, at 2 U.S.C. 1532, that agencies prepare an assessment of anticipated costs and benefits before issuing any rule that may result in the expenditure by State, local, and tribal Governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. This proposed rule would have no such effect on State, local, and tribal Governments or on the private sector.

List of Subjects

48 CFR Part 802, 804, 811, and 812

Government procurement.

48 CFR Part 824

Freedom of information, Government procurement, Privacy.

48 CFR Part 839

Computer technology, Government procurement.

48 CFR Part 852

Government procurement, Reporting and recordkeeping requirements.

Signing Authority

Denis McDonough, Secretary of Veterans Affairs, approved this document on October 12, 2021, and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.

***Consuela Benjamin**,*

Regulations Development Coordinator,
Office of Regulation Policy & Management,
Office of General Counsel,
Department of Veterans Affairs.

For the reasons set forth in the preamble, VA proposes to amend 48 CFR chapter 8 as follows:

PART 802—DEFINITIONS OF WORDS AND TERMS

1. The authority citation for part 802 is revised to read as follows:

Authority: 40 U.S.C. 121(c); 41 U.S.C. 1121; 41 U.S.C. 1303; 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

Subpart 802.1—Definitions

2. Section 802.101 is amended by adding definitions for “Business associate”, “Business Associate Agreement”, “Gray market items”, “Information system”, “Information technology”, “Information technology-related contracts”, “Privacy officer”, “Security plan”, “Sensitive personal information”, “VA Information Security Rules of Behavior for Organizational Users / VA National Rules of Behavior”, and “VA sensitive information” in alphabetical order to read as follows:

802.101 Definitions.

* * * * *

Business associate (or associate) means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another

covered entity, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191) Privacy Rule (45 CFR part 160) , that performs or assists in the performance of a function or activity on behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI), or that provides to or for VHA, certain services as specified in the HIPPA Privacy Rule (45 CFR part 160) that involve the disclosure of PHI to a contractor by VHA. The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI or that stores, generates, accesses, exchanges, processes, or utilizes such PHI on behalf of the business associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the HIPPA Privacy Rule (45 CFR part 160), between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA.

* * * * *

Gray market items means original equipment manufacturer goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

* * * * *

Information system means, pursuant to 38 U.S.C. 5727, a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

Information technology (*see* FAR 2.101), also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts which include

services (including support services) and related resources for information technology as defined in this section.

* * * * *

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual's identity, including but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records.

* * * * *

VA Information Security Rules of Behavior for Organizational Users / VA National Rules of Behavior means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various

confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

* * * * *

PART 804—ADMINISTRATIVE AND INFORMATION MATTERS

3.The authority citation for part 804 is revised to read as follows:

Authority: 38 U.S.C. 5723-5724; 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

4. Subpart 804.19 is added to read as follows:

Subpart 804.19—Basic Safeguarding of Covered Contractor Information Systems

Sec.

Subpart 804.19—Basic Safeguarding of Covered Contractor Information Systems

804.1900-70 Scope of this subpart.

This subpart prescribes policies and procedures for information security and protection of VA information, information systems, and VA sensitive information, including sensitive personal information.

804.1902 Applicability.

This subpart applies to all VA acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items, when a contractor's information system may contain VA information.

804.1970 Information security policy—contractor general responsibilities.

Contractors, subcontractors, business associates and their employees who are users of VA information or information systems, or have access to VA information and VA sensitive information shall—

(a) Comply with all VA information security and privacy program policies, procedures, practices and related contract requirements, specifications and clauses, this includes complying with VA privacy and confidentiality laws and implementing VA and VHA regulations (see 38 U.S.C. 5701, 5705, 5721-5728 and 7332; 38 CFR 1.460 through 1.496, 1.500 through 1.527, and 17.500 through 17.511), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 (as amended);

(b) Complete VA security awareness training on an annual basis;

(c) Complete VHA’s Privacy and Health Insurance Portability and Accountability Act of 1996 (HIPAA) Training on an annual basis when access to protected health information (PHI) is required;

(d) Report all actual or suspected security/privacy incidents and report the information to the contracting officer and contracting officer’s representative (COR), as identified in the contract or as directed in the contract, within one hour of discovery or suspicion;

(e) Comply with VA policy as it relates to personnel security and suitability program requirements for background screening of both employees and non-employees who have access to VA information systems and data;

(f) Comply with directions that may be issued by the contracting officer or COR, or from the VA Assistant Secretary for Information and Technology or a designated representative through the contracting officer or COR, directing specific activities when a security/privacy incident occurs;

(g) Sign an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723, FAR 39.105, Privacy, and clause 852.204-71, Information and Information Systems Security, on an annual basis. The VA Information Security Rules of Behavior describe the responsibilities and expected behavior of contractors, subcontractors, business associates and their employees who are users of VA information or information systems, information assets and resources, or have access to VA information;

(h) Maintain records and compliance reports regarding HIPAA Security and Privacy Rule compliance in order to provide such information to VA upon request to ascertain whether the business associate is complying with all applicable provisions under both rules' regulatory requirements; and

(i) Flow down requirements in all subcontracts and Business Associate Agreements (BAAs), at any level, as provided in the clause at 852.204-71, Information and Information Systems Security.

804.1903 Contract clause.

When the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903, the

contracting officer shall insert clause 852.204-71, Information and Information Systems Security.

PART 811—DESCRIBING AGENCY NEEDS

5. The authority citation for part 811 is revised to read as follows:

Authority: 38 U.S.C 5723-5724; 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1303; 1702 and 48 CFR 1.301 through 1.304.

6. Subpart 811.5 is added to read as follows:

Subpart 811.5—Liquidated Damages

Sec.

Subpart 811.5—Liquidated Damages

811.500 Scope.

This subpart prescribes policies and procedures for using a liquidated damages clause in solicitations and contracts that involve VA sensitive personal information. This also pertains to any solicitations and contracts involving VA sensitive personal information issued by another agency for or on behalf of VA through an interagency acquisition in accordance with FAR subpart 17.5 and subpart 817.5.

811.501-70 Policy—statutory requirement.

(a) Contracting officers are required to include a liquidated damages clause in contracts for the performance of any Department function which requires access to VA sensitive personal information (see the definition in 802.101), in accordance with 38 U.S.C. 5725(b). The liquidated damages are to be paid by the contractor to the Department of Veterans Affairs in the event of a data breach involving sensitive

personal information maintained, processed, or utilized by contractors or any subcontractors.

(b) The purpose of the liquidated damages to be paid for by the contractor in the event of a data breach of personal sensitive information is for VA to provide credit protection services to affected individuals pursuant to 38 U.S.C. 5724(a)-(b).

811.503-70 Contract clause.

(a) Insert the clause at 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs, in all solicitations, contracts, or orders, where VA requires access to sensitive personal information for the performance of a Department function where—

(1) Sensitive personal information (see 802.101, Definitions) will be created, received, maintained, or transmitted, or that will be stored, generated, accessed, or exchanged such as protected health information (PHI) or utilized by a contractor, subcontractor, business associate, or an employee of one of these entities; or,

(2) When VA information systems will be designed or developed at non-VA facilities where such sensitive personal information is required to be created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized.

(b) Insert the clause at 852.211-76 with its Alternate I in all solicitations, contracts, or orders, in commercial items acquisitions awarded under the procedures of FAR part 8 or 12.

(c) Insert the clause at 852.211-76 with its Alternate II, in all solicitations, contracts, or orders, in simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial items awarded under the procedures of FAR part 13 (see FAR 13.302-5(d)(1) and the clause at FAR 52.213-4).

PART 812—ACQUISITION OF COMMERCIAL ITEMS

7. The authority citation for part 812 continues to read as follows:

Authority: 38 U.S.C. 8127-8128; 40 U.S.C. 121(c); 41 U.S.C. 1702 and 48 CFR 1.301 through 1.304.

Subpart 812.3—Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items

8. Section 812.301 is revised to read as follows:

812.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

(f)(1) Contracting officers shall insert the clause 852.212-71, Gray Market and Counterfeit Items, in solicitations and contracts for new medical supplies, new medical equipment, new information technology equipment, and maintenance of medical or information technology equipment that includes replacement parts if used, refurbished, or remanufactured parts are unacceptable, when the associated solicitation includes FAR provisions 52.212-1 Instruction to Offerors-Commercial Items, and 52.212-2, Evaluation-Commercial Items.

(2) Contracting officers shall insert the clause 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts, in solicitations and contracts for the maintenance of information technology equipment that includes replacement parts, if used, refurbished, or remanufactured parts are acceptable, when the associated solicitation includes FAR provisions 52.212-1, Instruction to Offerors-Commercial Items, and 52.212-2, Evaluation-Commercial Items.

PART 824—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

9. The authority citation for part 824 is revised to read as follows:

Authority: 5 U.S.C. 552a; 38 U.S.C. 5723-5724; 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1121(c); 41 U.S.C. 1702; 38 CFR 1.550 through 1.562 and 1.575 through 1.584; and 48 CFR 1.301 through 1.304.

Subpart 824.1— Protection of Individual Privacy

10. Sections 824.103-70 and 824.103-71 are added to read as follows:

824.103-70 Protection of privacy—general requirements and procedures related to Business Associate Agreements.

To ensure compliance with unique responsibilities to protect protected health information, contractors performing under VA contracts subject to unique protected health information (PHI) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall comply with requirements and the clause prescribed at 804.1903, 852.204-71, Information and Information Systems Security.

(a) *HIPAA Business Associate Agreement requirement*. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, a Covered Entity (Veterans Health Administration (VHA)) must have a satisfactory assurance that its protected health information will be safeguarded from misuse. To do so, a Covered Entity enters into a Business Associate Agreement (BAA) with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's protected health information for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same disclosure restrictions to PHI that is required of the Covered Entity in situations where a contractor —

(1) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the Covered Entity; or

(2) Provides one or more of the services specified in the HIPPA Privacy Rule to or for the Covered Entity.

(b) *Veterans Health Administration (VHA)—a HIPAA Covered Entity*. VHA is the only administration of the Department of Veterans Affairs that is a HIPAA Covered Entity under the HIPAA Privacy Rule.

(c) *Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates.* BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA.

(1) There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(2) Contractors or other entities supporting VHA required to create, receive, maintain, or transmit VHA PHI shall be required to execute a BAA as mandated by the Privacy Rule and requested by the contracting officer, the contracting officer's representative (COR) or the cognizant privacy officer—

(i) Whether via a contract or agreement with VHA; or

(ii) Whether provided from or through another VA administration or staff activity contract for supplies, services or support that involves performing a certain activity, function or service to, for, or on behalf of VHA (*see* VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management).

(d) *BAA requirement flow down to subcontractors*. A prime contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with

HIPAA requirements to the same degree as the contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (*i.e.*, also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the Covered Entity and the prime contractor.

824.103-71 Liquidated damages—protection of information.

(a) *Purpose*. As required by 38 U.S.C. 5725 any contracts where sensitive personal information such as protected health information (PHI) must be disclosed to the contractor for the contractor to perform certain functions or services on behalf of VHA shall include a liquidated damages clause as prescribed at 811.503-70.

(b) *Applicability to contracts requiring Business Associate Agreements*. A liquidated damages clause is required (*see* 811.503-70) when performance under a contract requires a contractor to enter into a Business Associate Agreement with VHA because the contractor or its subcontractor is required to create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI, for certain services or functions, on behalf of VHA. The liquidated damages clause shall be added even in situations where the prime contractor never directly receives VA's sensitive personal information and the same flows directly to the prime contractor's subcontractor.

11. Part 839 is added to read as follows:

PART 839—ACQUISITION OF INFORMATION TECHNOLOGY

Sec.

839.000 Scope of part.

Subpart 839.1—General

Subpart 839.2—Information and Communication Technology

Authority**:** 38 U.S.C. 5723-5724; 5725(a)–(c); 40 U.S.C. 121(c); 40 U.S.C. 11319(b)(1)(C); 41 U.S.C. 1121(c)(3); 1303 and 1702; and 48 CFR 1.301 through 1.304.

839.000 Scope of part.

This part prescribes acquisition policies and procedures for use in acquiring VA information technology and information technology-related contracts (see 802.101) and applies to both VA-procured information technology systems as well as Interagency Acquisitions defined in FAR part 17 and part 817.

Subpart 839.1—General

839.101 Policy.

(a)(1) In acquiring information technology, including information technology-related contracts which may involve services (including support services), and related resources (*see* the definition at FAR 2.101), contracting officers and requiring activities shall include in solicitations and contracts the requirement to comply with the following directives, policies, and procedures in order to protect VA information, information systems, and information technology—

(i) VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series, to include, but not limited to, VA Handbook 6500.6, Contract Security, which establishes VA's procedures, responsibilities, and processes

for complying with current Federal law, Executive orders, policies, regulations, standards and guidance for protecting and controlling VA sensitive information and ensuring that security requirements are included in acquisitions, solicitations, contracts, purchase orders, and task or delivery orders.

(ii) The VA directives, security requirements, procedures, and guidance in paragraph (a)(1)(i) of this section apply to all VA contracts and to contractors, subcontractors, and their employees in the performance of contractual obligations to VA for information technology products purchased from vendors, as well as for services acquired from contractors and subcontractors or business associates, through contracts and service agreements, in which access to VA information, VA sensitive information or sensitive personal information (including protected health information (PHI))—

(A) That is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized by VA, a VA contractor, subcontractor or third-party servicers or associates, or on behalf of any of these entities, in the performance of their contractual obligations to VA; and

(B) By or on behalf of any of the entities identified in this section, regardless of—

(*1*) Format; or

(*2*) Whether it resides on a VA or a non-VA system, or with a contractor, subcontractor, or third-party system or electronic information system(s), including cloud services, operating for or on the VA's behalf or as required by contract.

(c) Contractors, subcontractors, and third-party servicers or associates providing support to or on behalf of these entities, shall employ adequate security controls and use appropriate common security configurations available from the National Institute of Standards and Technology (*see* FAR 39.101(c)) as appropriate in accordance with VA regulations, directives, handbooks and guidance, and established service level agreements and individual contracts, orders, and agreements. Contractors,

subcontractors, and third-party servicers and associates will ensure that VA information or VA sensitive information that resides on a VA system or resides on a contractor/subcontractor/third-party entities/associates information and communication technology (ICT) system(s), operating for or on VA's behalf, or as required by contract, regardless of form or format, whether electronic or manual, and information systems, are protected from unauthorized access, use, disclosure, modification, or destruction to ensure information security (see FAR 2.101) is provided in order to ensure the integrity, confidentiality, and availability of such information and information systems.

839.105 Privacy.

839.105-70 Business Associate Agreements, information technology-related contracts and privacy.

In accordance with 824.103-70, Protection of privacy—general requirements and procedures related to Business Associate Agreements, contracting officers and contracting officer representatives (CORs) shall ensure that contractors, their employees, subcontractors and third-parties under the contract complete Business Associate Agreements for—

(a) Information technology or information technology-related service contracts subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) where HIPAA protected health information (PHI) is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized in order to perform certain health care operations activities or functions on behalf of the Veterans Health Administration (VHA) as a covered entity (see 802.101 for the definition of information technology-related contracts); or

(b) Contractors supporting other VA organizations which support VHA in this regard and which would therefore require Business Associate Agreements in accordance with 824.103-70.

839.105-71 Liquidated damages—protection of information in information technology related contracts.

Contracting officers shall insert in information technology related contracts the liquidated damages clause as prescribed at 811.503-70.

839.106-70 Information technology security and privacy clauses.

(a) Contracting officers shall insert the clause at 852.239-70, Security Requirements for Information Technology Resources, and the clause 852.239-71, Information Technology Security Plan and Accreditation, in all solicitations, contracts, and orders exceeding the micro-purchase threshold that include information technology services.

(b) Contracting officers shall insert the clause at 852.239-72, Information System Design and Development, in solicitations, contracts, orders, and agreements where services to perform information system design and development are required.

(c) Contracting officers shall insert the clause at 852.239-73, Information System Hosting, Operation, Maintenance or Use, in solicitations, contracts, orders, and agreements where services to perform information system hosting, operation, maintenance, or use are required.

(d) Contracting officers shall insert the clause at 852.239-74, Security Controls Compliance Testing, in solicitations, contracts, orders, and agreements, when the clauses at 852.239-72 or 852.239-73 are inserted.

Subpart 839.2—Information and Communication Technology

839.201 Scope of subpart.

This subpart applies to the acquisition of Information and Communication Technology (ICT) supplies and services. It concerns the access to and use of information and data, by both Federal employees with disabilities, and members of the public with disabilities in accordance with FAR 39.201. This implements VA policy on

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and 36 CFR parts 1193 and 1194 as it applies to contracts and acquisitions when developing, procuring, maintaining or using ICT.

839.203 Applicability.

(a) *General*. Solicitations for information technology (i.e., information and communication technology (ICT)) or IT-related supplies and services shall require the contractor to submit a VA Section 508 Checklist (*see* http://www.section508.va.gov/).

839.203-70 Information and communication technology accessibility standards—contract clause and provision.

(a) The contracting officer shall insert the provision at 852.239-75, Information and Communication Technology Accessibility Notice, in all solicitations.

(b) The contracting officer shall insert the clause at 852.239-76, Information and Communication Technology Accessibility, in all contracts and orders.

PART 852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

12. The authority citation for part 852 continues to read as follows:

Authority: 38 U.S.C. 8127-8128, and 8151-8153; 40 U.S.C. 121(c); 41 U.S.C. 1121(c)(3), 41 U.S.C. 1303; 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

Subpart 852.2—Texts of Provisions and Clauses

13. Section 852.204-71 is added to read as follows:

852.204-71 Information and Information Systems Security.

As prescribed in 804.1903 insert the following clause:

INFORMATION AND INFORMATION SYSTEMS SECURITY (DATE)

(a) *Definitions*. As used in this clause—

Business Associate means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another covered entity, as defined by the Health Insurance Portability and Accountability Act of

1996 (HIPAA) Privacy Rule, that performs or assists in the performance of a function or activity on behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI). The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the Privacy Rule, between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

Information technology (*see* FAR 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts which include services (including support services), and related resources for information technology as defined in 802.101.

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual’s

identity, including but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records.

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or

could adversely affect the national interest or the conduct of Federal programs.

(b) *General*. Contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, *Personnel Security and Suitability Program*, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (*see* 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(c) *Access to VA information and VA information systems*. (1) Contractors are limited in their request for logical or physical access to VA information or VA information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors to access VA information and VA information systems shall be in accordance with VA Directive and Handbook 0710, *Personnel Security and Suitability Program*.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) HIPAA Business Associate Agreement requirement. Contractors shall enter into a Business Associate Agreement with VHA, VA's Covered Entity, when contract requirements and access to protected health information is required and when requested by the Contracting Officer, or the Contracting Officer's Representative (COR) (see VAAR 824.103-70). Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, a Covered Entity (Veterans Health Administration) must have a satisfactory assurance that its protected health information will be safeguarded from misuse. To do so, a Covered Entity enters into a Business Associate Agreement (BAA) with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's protected health information for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same disclosure restrictions to protected health information (PHI) that is required of the Covered Entity in situations where a contractor—

(i) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the Covered Entity; or

(ii) Provides one or more of the services specified in the Privacy Rule to or for the Covered Entity.

(A) *Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates.* BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such

PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA. There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(B) *BAA requirement flow down to subcontractors*. A prime Contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the Contractor. Contractors employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the Covered Entity and the prime Contractor.

(d) *Contractor operations required to be in United States*. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other VA policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable Business Associate Agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the

Contractor/subcontractor must include a detailed Information Technology Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) *Contractor/subcontractor employee reassignment and termination notification*. Contractors and subcontractors shall provide written notification to the Contracting Officer and Contracting Officer's Representative (COR) immediately, and not later than four (4) hours, when an employee working on a VA information system or with access to VA information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant VA contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(f) *VA information custodial requirements*. (1) *Release, publication, and use of data*. Information made available to a Contractor or subcontractor by VA for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without VA's prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in Rights in Data—General, FAR 52.227-14(d).

(2) *Media sanitization*. VA information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and VA requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (*see* VA Directive 6500, VA Cybersecurity Program). VA reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and VA requirements. The

Contractor and subcontractor will provide all necessary access and support to VA and/or GAO staff during periodic control assessments or audits.

(3) *Data retention, destruction and contractor self-certification*. The Contactor and its subcontractors are responsible for collecting and destroying any VA data provided, created, or stored under the terms of this contract, to a point where VA data or materials are no longer readable or reconstructable to any degree, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, or subsequent issue. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction of all VA data in its possession according to VA Handbook 6500, and VA Cybersecurity Program, including compliance with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) *Return of VA data and information*. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VA (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying BAA. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract using VA-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or

equipment will be destroyed unless done in accordance with the terms of this contract and the VHA Records Control Schedule 10-1.

(5) *Use of VA data and information*. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if the National Institute of Standards and Technology (NIST) issues or updates applicable Federal Information Processing Standards (FIPS) or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) *Copying VA data or information*. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) *Violation of information custodial requirements*. If VA determines that the Contractor has violated any of VA's information confidentiality, privacy, or security provisions, it shall be sufficient grounds for VA to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) *Encryption*. The Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract, using cryptography, and VA-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) *Firewall and web services security controls*. The Contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

(10) *Disclosure of VA data and information*. Except for uses and disclosures of VA information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose VA information only in two other situations: (i) subject to paragraph 10 of this section, in response to a court order from a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/ subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose VA information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of VHA, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and

Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated VA facility Privacy Officer as provided in the contract, BAA, or by the Contracting Officer. If providing the Accounting of disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) *Compliance with privacy statutes and applicable regulations*. The Contractor/subcontractor shall not disclose VA information protected by any of VA's privacy statutes or applicable regulations including but not limited to: the Privacy Act of 1974, 38 U.S.C. 5701, confidential nature of claims, 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus or the HIPAA Privacy Rule. If the Contractor/subcontractor is in receipt of a court order or other requests for VA information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(g) *Report of known or suspected security/privacy incident*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR or within one (1) hour of an incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use

policies. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. See VA Data Breach Response Service at https://www.oprm.va.gov/dbrs/about_dbrs.aspx. Report all actual or suspected security/privacy incidents and report the information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than _____ days [*Fill in: Contracting Officer fills in the number of days*]. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (*e.g.*, Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within ____ [*Fill in: Contracting Officer fills in the number of days in consultation with requiring activity*].

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, but within 60 days of discovery or disclosure. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of VA) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology. These exceptions will be tracked by the Contractor in concert with the Government in accordance with VA Directive 6500.6 and related VA Handbooks.

(h) *Security and privacy incident investigation*. (1) The term “privacy incident” means the unauthorized disclosure or use of VA information protected under a confidentiality statute or regulation. (2) The term "security incident" means an

occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies. The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected security or privacy incident, or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the Business Associate is deemed to have discovered a security incident as defined above when the Business Associate either knew, or by exercising reasonable diligence should have been known to an employee of the Business Associate. Upon discovery, the Business Associate must notify VHA of the security incident immediately within one hour of discovery or suspicion as agreed to in the Business Associate Agreement (BAA).

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other

compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(i) *Data breach notification requirements*. (A) This contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

(B) The Contractor/subcontractor shall -provide notice to VA of a privacy or security incident as set forth in the Security and Privacy Incident Investigation section of this clause. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

(C) The Contractor/subcontractor shall fully cooperate with VA or any Government agency conducting an analysis regarding any notice of a data breach or potential data breach or security incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for VA, and shall address all relevant information concerning the data breach, including the following:

(*1*) Nature of the event (loss, theft, unauthorized access).

(*2*) Description of the event, including—

(*i*) Date of occurrence;

(*ii*) Date of incident detection;

(*iii*) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(*iv*) Number of individuals affected or potentially affected.

(*v*) Names of individuals or groups affected or potentially affected.

(*vi*) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(*vii*) Amount of time the data has been out of VA control.

(*viii*) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).

(*ix*) Known misuses of data containing sensitive personal information, if any.

(*x*) Assessment of the potential harm to the affected individuals.

(*xi*) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate.

(*xii*) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(*xiii*) Steps taken in response to mitigate or prevent a repetition of the incident.

(j) *Training*. (1) All Contractor employees and subcontractor employees requiring access to VA information or VA information systems shall complete the following before being granted access to VA information and its systems:

(i) On an annual basis, successfully complete the VA Privacy and Information Security Awareness and VA Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior for Organizational Users, relating to access to VA information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that VA Information Security Rules of Behavior for Organizational Users signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the VA Information Security Rules of Behavior, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(k) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and business associate agreements, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to VA information (including VA sensitive information, *i.e.*, sensitive personal information and protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see VAAR 802.101 definition of information technology-related contracts.)

(End of clause)

14. Section 852.211-76 is added to read as follows:

852.211-76 Liquidated Damages—Reimbursement for Data Breach Costs.

As prescribed in 811.503-70, Contract clause, insert the following clause:

LIQUIDATED DAMAGES—REIMBURSEMENT FOR DATA BREACH COSTS (DATE)

(a) *Definition*. As used in this clause, “contract” means any contract, agreement, order or other instrument and encompasses the definition set forth in FAR 2.101.

(b) *Non-disclosure requirements*. As a condition of performance under a contract, order, agreement, or other instrument that requires access to sensitive personal information as defined in VAAR 802.101, the following is expressly required—

(1) The Contractor, subcontractor, their employees or business associates shall not, directly or through an affiliate or employee of the Contractor, subcontractor, or business associate, disclose sensitive personal information to any other person unless the disclosure is lawful and is expressly permitted under the contract; and

(2) The Contractor, subcontractor, their employees or business associates shall immediately notify the Contracting Officer and the Contracting Officer’s Representative (COR) of any security incident that occurs involving sensitive personal information.

(c) *Liquidated damages*. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of _____ [*Contracting Officer insert amount*] per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. In the event the Contractor provides payment of actual damages in an amount determined to be adequate by the Contracting Officer, the Contracting Officer may forgo collection of liquidated damages.

(d) *Purpose of liquidated damages*. Based on the results from VA’s determination that there was a data breach caused by Contractor’s or any of its agents’ failure to protect or otherwise engaging in conduct to cause a data breach of VA sensitive personal information, and as directed by the Contracting Officer, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of _____ [*Contracting Officer insert amount*] per affected individual to cover the cost of the

following:

(1) Notification related costs

(2) Credit monitoring reports.

(3) Data breach analysis and impact.

(4) Fraud alerts.

(5) Identity theft insurance.

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract, purchase order, or agreement, in whole or in part under clause 52.249-8, Default—Fixed-Price Supply and Service, or any other related FAR or VAAR clause included in the contract, in addition to the required liquidated damages for data breach-related expenses specified in paragraph (c) above, the Contractor is liable for excess costs for those supplies and services for repurchase as may be required under the Termination clause.

(End of clause)

Alternate I (DATE). In commercial items acquisitions awarded under the procedures of FAR part 8, or FAR part 12, substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.212-4(m), Contract Terms and Conditions—Commercial Items, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

Alternate II (DATE). In simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial items awarded under the procedures of

FAR part 13 (*see* FAR 13.302-5(d)(1) and the clause at FAR 52.213-4), substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.213-4(g), Terms and Conditions – Simplified Acquisitions (Other Than Commercial Items), or any other applicable FAR or VAAR clause, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

852.212-70 [Removed and Reserved]

15. Section 852.212-70 is removed and reserved.

16. Section 852.212-71 is revised to read as follows:

852.212-71 Gray Market and Counterfeit Items.

As prescribed in 812.301(f), insert the following clause:

GRAY MARKET AND COUNTERFEIT ITEMS (DATE)

(a) No used, refurbished, or remanufactured supplies or equipment/parts shall be provided. This procurement is for new Original Equipment Manufacturer (OEM) items only. No gray market items shall be provided. Gray market items are OEM goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

(b) No counterfeit supplies or equipment/parts shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items

represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

(c) Vendor shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

(End of clause)

17. Section 852.212-72 is added to read as follows:

852.212-72 Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts.

As prescribed in 812.301(f), insert the following clause:

GRAY MARKET AND COUNTERFEIT ITEMS—INFORMATION TECHNOLOGY MAINTENANCE ALLOWING OTHER-THAN-NEW PARTS (DATE)

(a) Used, refurbished, or remanufactured parts may be provided. No gray market supplies or equipment shall be provided. Gray market items are Original Equipment Manufacturer (OEM) goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

(b) No counterfeit supplies or equipment shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

(c) Vendor shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

(End of clause)

18. Section 852.239-70 is added to read as follows:

852.239-70 Security Requirements for Information Technology Resources.

As prescribed in 839.106-70, insert the following clause:

SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (DATE)

(a) *Definitions*. As used in this clause—

Information technology has the same meaning in FAR 2.101 and also *means* Information and Communication Technology (ICT).

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) *Responsibilities*. The Contractor shall be responsible for information technology security for all systems connected to a Department of Veterans Affairs (VA) network or operated by the Contractor for VA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to VA information that directly supports the mission of VA. Examples of tasks that require security provisions include—

(1) Hosting of VA e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by VA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to VA general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) *Information technology security plan*. The Contractor shall develop, provide, implement, and maintain an Information Technology Security Plan. VA information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information technology resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, PIA, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The plan shall address the specific contract requirements regarding information technology and information technology-related support or services included in the contract, to include the PWS or SOW. The Contractor's Information Technology Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information technology security requirements in accordance with Federal and VA policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following.

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines; and

(3) VA Directive 6500, VA Cybersecurity Program, and the directives and

handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(d) *Submittal of plan*. Within 30 days after contract award, the Contractor shall submit the Information Technology Security Plan to the Contracting Officer for review and approval.

(e) *Security accreditation*. As required by current VA policy, the Contractor shall submit written proof of information technology security accreditation to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with VA policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this accreditation a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and accompanying documents, to include a final security plan, risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan.

(f) *Annual validation*. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.

(g) *Banners*. The Contractor shall ensure that the official VA banners are

displayed on all VA systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system. The Office of Information Technology will make official VA banners available to the Contractor.

(h) *Screening and access*. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for VA or interconnected to a VA network in accordance with VA Directives and Handbooks referenced in paragraph (c).

(i) *Training*. The Contractor shall ensure that its employees performing services under this contract complete VA security awareness training on an annual basis. This includes signing an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723; FAR 39.105, Privacy; clause 852.204-71, Information and Information Systems Security, and this clause on an annual basis.

(j) *Government access*. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information technology inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of VA data or to the function of information technology systems operated on behalf of VA), and to preserve evidence of computer crime.

(k) *Notification of termination of employees*. The Contractor shall immediately notify the Contracting Officer when an employee who has access to VA information systems or data terminates employment.

(l) *Subcontractor flow down requirement*. The Contractor shall incorporate and

flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

19. Section 852.239-71 is added to read as follows:

852.239-71 Information Technology Security Plan and Accreditation.

As prescribed in 839.106-70, insert the following provision:

INFORMATION TECHNOLOGY SECURITY PLAN AND ACCREDITATION (DATE)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 852.239-70, Security Requirements for Information Technology Resources.

(End of provision)

20. Section 852.239-72 is added to read as follows:

852.239-72 Information System Design and Development.

As prescribed in 839.106-70, insert the following clause:

INFORMATION SYSTEM DESIGN AND DEVELOPMENT (DATE)

(a) *Design or development at non-VA facilities*. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with the Federal Information Security Modernization Act of 2014 and Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA) regulations, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199

system security categorization and the Trusted Internet Connections (TIC) Reference Architecture).

(b) *Privacy Impact Assessment*. During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

(c) *Security of procured or developed systems and technologies*. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that Security Fixes shall not negatively impact the Systems.

(d) *Subcontract flow down requirements*. (1) The Contractor shall include the clause at 52.224-1, Privacy Act Notification, in every solicitation and/or subcontract awarded by the Contractor when the clause FAR 52.224-1 is included in its contract.

(End of clause)

21. Section 852.239-73 is added to read as follows:

852.239-73 Information System Hosting, Operation, Maintenance, or Use.

As prescribed in 839.106-70, insert the following clause:

INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE (DATE)

(a) Definitions. As used in this clause—

Assessment and Authorization (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have

effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable VA policies and procedures is the mechanism by which VA provides an Authorization to Operate (ATO), the official management decision given by the VA to authorize operation of an information system (see VA Handbook 6500 for additional details).

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) *Hosting, operation, maintenance, or use at non-VA facilities*. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy handbooks, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent to or exceed, those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to approval to operate. All external Internet connections to VA's network involving VA information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) *Collecting, processing, transmitting, and storing of PII*. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the Privacy Impact Assessment and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

(d) *Annual FISMA security controls assessment*. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the Privacy Impact Assessment. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into VA's POA&M management process. The Contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the VA in the performance work statement or statement of work, or in the approved remediation plan through the VA POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500. This may

require reviewing and updating all of the documentation as described in VA Handbook 6500.6 (e.g., System Security Plan, Contingency Plan). See VA Handbook 6500.6 for a list of documentation. The VA Information System Risk Management (ISRM) office can provide guidance on whether a new A&A would be necessary.

(e) *Annual self-assessment*. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. VA reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) *Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on VA networks*. VA prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on VA networks. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, PWS, SOW or contract. All of the security controls required for government furnished equipment (GFE) must also be utilized in approved other equipment (OE) at the Contractor's expense. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

(g) *Disposal or return of electronic storage media on non-VA leased or non-VA owned IT equipment*. All electronic storage media used on non-VA leased or non-VA

owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA directives and handbooks upon—

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (*e.g.*, hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per VA Handbook 6500.1 requirements. This must be completed within 30 days of termination of the contract.

(h) *Bio-Medical devices and other equipment or systems*. Bio-Medical devices and other equipment or systems containing media (*e.g.*, hard drives, optical disks) with VA sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of VA sensitive information the devices may be provided back to the Contractor under one of three scenarios—

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn-in if VA's initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

22. Section 852.239-74 is added to read as follows:

852.239-74 Security Controls Compliance Testing.

As prescribed in 839.106-70(d), insert the following clause:

SECURITY CONTROLS COMPLIANCE TESTING (DATE)

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by VA in the event of a security incident or at any other time.

(End of clause)

23. Section 852.239-75 is added to read as follows:

852.239-75 Information and Communication Technology Accessibility Notice.

As prescribed in 839.203-70(a), insert the following provision:

INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (DATE)

(a) Any offeror responding to this solicitation must comply with established VA Information and Communication Technology (ICT) (formerly Electronic and Information (EIT)) accessibility standards. Information about Section 508 is available at http://www.section508.va.gov/.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 852.239-75, Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit appropriate VA Section 508 Checklists, in accordance with the checklist completion instructions. The purpose of the checklists is to assist VA acquisition and program

officials in determining whether proposed ICT supplies, or information, documentation and services conform to applicable Section 508 accessibility standards. The checklists allow offerors or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues.

(c) Respondents to this solicitation must identify any exception to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(End of provision)

24. Section 852.239-76 is added to read as follows:

852.239-76 Information and Communication Technology Accessibility.

As prescribed in 839.203-70(b), insert the following clause:

INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (DATE)

(a) All information and communication technology (ICT) (formerly referred to as electronic and information technology (EIT)) supplies, information, documentation and services support developed, acquired, maintained or delivered under this contract or order must comply with the ‘‘Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards’’ (*see* 36 CFR part 1194). Information about Section 508 is available at http://www.section508.va.gov/.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the specification, statement of work, or performance work statement. If it

is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are: _____ [*Contracting Officer: insert the applicable Section 508 accessibility standards*].

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the Contractor submit a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the

level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

[FR Doc. 2021-24299 Filed: 11/16/2021 8:45 am; Publication Date: 11/17/2021]